IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: **Black iPhone, currently located at 12200 Sunrise Valley Drive, Reston, VA 20191**	Case No. 1:24-SW-160

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Andrew Speights, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I made this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the black iPhone, further described in Attachment A and referred to as "the iPhone." This item was recovered from the defendant's (Tony Mauricio VIERA) possession during a search incident to arrest on February 14, 2024 within the Eastern District of Virginia.

2. I am a Task Force Officer (TFO) with Homeland Security Investigations (HSI) in Reston, Virginia. I am an investigator or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered to conduct investigations and to make arrests. I have been a Task Force Officer with HSI since 2019. During this time, I completed the HSI Title 19 training course for TFOs. I am also currently assigned to a unit that investigates violent gangs at the Washington, D.C. Special Agent in Charge Office.

3. I have been a sworn Law Enforcement Officer in the Commonwealth of Virginia for over twelve (12) years and currently work for the Manassas City Police Department's Investigative Services Division. I have received training from a state approved Criminal Justice Academy as well as in-service training which covered many police related skills, techniques, and legal matters. Additionally, I have made numerous arrests that have been successfully prosecuted in Prince William County Circuit Court and have been trained and involved in the successful execution of search warrants in this and other jurisdictions in the Northern Virginia region.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested search warrant and does not set forth all my knowledge about this matter. I base this information based upon facts I learned as well as from information gathered by other law enforcement personnel.

5. Tony Mauricio VIERA ("VIERA"), is charged with illegal re-entry after removal subsequent to a felony conviction, in violation of Title 8, U.S.C., Section 1326. I believe there is probable cause to believe that a search of the iPhone located on his person at the time of his arrest will reveal evidence relating to his illegal entry as well as being an unregistered sex offender in violation of 18 U.S.C. §2250 as more particularly described in Attachment B.

PROBABLE CAUSE

6. HSI is investigating VIERA for failing to register or update a registration as a sex offender in violation of Title 18, U.S.C., Section 2250(a) in addition to being a removed alien found in the United States in violation 8 U.S.C. §1326.

7. VIERA is a citizen and national of El Salvador who was previously removed from the United States on or about February 10, 2020, at or near Alexandria, Louisiana. Prior to his first removal on or about February 10, 2020, VIERA was convicted of Carnal Knowledge of a Minor (VA Code 18.2-63), in Prince William Circuit Court, Virginia on December 15, 2016. As a result of this 2016 conviction, VIERA was classified as a sex offender under Virginia law and was required to register as a sex offender for life with the Virginia Department of State Police.

8. VIERA was issued the Sex Offender and Crimes Against Minors Registry Order of Remand, in Virginia on December 15, 2016, while in custody on his conviction for Carnal Knowledge of a Minor. At that time, VIERA signed his Order of Remand – Sex Offender and Crimes Against Minors Registry form, ("Registration form") acknowledging his duty to register. VIERA's Registration form also informed VIERA of his future registration requirements, which were provided on the Registration form in both English and Spanish. Per the Registration form and Virginia state law, VIERA was required to register within three (3) days from the date of sentencing or if he was to return to Virginia.

9. Subsequently, VIERA was deported for the first time on or about February 10, 2020. VIERA voluntarily and unlawfully re-entered the United States on an unknown date and was found in the Eastern District of Virginia in early 2024. On or about January 18, 2024, I observed VIERA in the United States and within the Eastern District of Virginia, at the residence located at 7411 Peppertree Lane, Manassas, VA 20111. VIERA was later arrested at this location on or about February 14, 2024.

10. There was no record of VIERA having ever registered with the Commonwealth of Virginia as a sex offender. Further, a query of the National Sex Offender Public Website indicated VIERA was not lawfully registered in any other jurisdiction.

11. Per the Commonwealth of Virginia Department of State Police, VIERA is a sex offender based on his Carnal Knowledge of a Minor conviction in Prince William County, Virginia. As a sex offender, VIERA is required to register as a Sex Offender within three days of establishing residency in Virginia, must update his registration every ninety days, and must remain on the sex offender registry for life. I believe VIERA failed to register or update a registration as required by the Sex Offender Registration and Notification Act.

12. On or about February 14, 2024, a black iPhone, described in Attachment A was recovered during search incident to arrest of VIERA for violation of Title 8, U.S.C., Section 1326. VIERA later confirmed ownership of the iPhone.

13. I believe that there is probable cause to believe that evidence, fruits, or contraband can be found on the iPhone that will help establish that VIERA has been residing within the United States post removal, and more specifically within the Eastern District of Virginia for more than 30 days prior to his arrest in February 2024 for illegal entry. I know that electronic devices can contain photographs with geolocation data, helping establish length of residence, and text messages regarding meeting up with individuals in the area or discussing locations that establish that an individual is residing in the area. Individuals will often communicate their addresses to others via text message and will discuss subjects that indicate where they reside.

ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

14. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on devices. This information can sometimes be recovered with forensics tools.

15. There is probable cause to believe that things that were once stored on the iPhone may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has

been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

16. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the iPhone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the iPhone because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the

times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the iPhone consistent

with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the iPhone to human inspection in order to determine whether it is evidence described by the warrant.

18. Manner of execution. Because this warrant seeks only permission to examine the iPhone which is already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

For the reasons stated above, there is probable cause to believe that VIERA, has not registered as a sex offender as required by law after having lived in the Eastern District of Virginia for more than 30 days. Further, there is probable cause to believe that the iPhone contains evidence of these crimes, including (but not limited to) information confirming his domicile and location over the past thirty days or more.

Respectfully submitted,

Andrew Speights
HSI Task Force Officer
U.S. Immigration and Customs Enforcement

Subscribed and sworn to in accordance

with Fed. R. Crim. P. 4.1 by telephone

on March 8, 2024

Lindsey R Vaala

Digitally signed by Lindsey R Vaala
Date: 2024.03.08 11:48:32 -05'00'

THE HONORABLE LINDSEY R. VAALA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is the following device currently located at the HSI DC SAC office at 12200 Sunrise Valley Drive, Reston, Virginia:

1. a black Apple iPhone which was recovered from Tony VIERA's person during a search incident to VIERA's arrest on February 14, 2023.

This warrant authorizes the forensic examination of the iPhone for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Information/Items to be Searched for and Seized

2. All records relating to violations of Title 18 U.S.C. § 2250(a), those violations involving VIERA, for the iPhone described in Attachment A including:

a. Records and information relating to location, dates of access of the iPhone indicating VIERA's presence in Virginia;

b. Records and information relating to the location of VIERA from February 11, 2020 to February 14, 2024;

c. Records and information relating to the length of time VIERA has resided in Virginia and to where he resided specifically during that time between February 11, 2020 and February 14, 2024;

d. Text messages containing information about his location or residence or failure to register between February 11, 2020 and February 14, 2024;

e. Photographs that contain evidence of location or residence between February 11, 2020 and February 14, 2024;

f. evidence of who used, owned, or controlled the iPhone at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

g. evidence indicating how and when the iPhone was accessed or used to determine the chronological context of iPhone access, use, and events relating to crime under investigation and to the user;

h. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the iPhone;

i. evidence of the times the iPhone was used and by whom;

j. passwords, encryption keys, and other access devices that may be necessary to access the iPhone;

k. records of or information about Internet Protocol addresses used by the iPhone;

l. records of or information about the iPhone's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.